Diophantine sets of polynomials over number fields

Jeroen Demeyer*

2008–09–11

Abstract

Let $\mathcal{R}$ be a recursive subring of a number field. We show that recursively enumerable sets are diophantine for the polynomial ring $\mathcal{R}[Z]$.

2000 MSC: 11D99 (primary), 03D25, 12L12, 11R09, 12E10 (secondary).
Keywords: Diophantine set, Recursively enumerable set, Hilbert's Tenth Problem.

1 Introduction

Let $\mathcal{R}$ be a recursive subring of a number field. In this paper, we show that recursively enumerable (r.e.) subsets of $\mathcal{R}[Z]^k$ are diophantine.

For any recursively stable integral domain, one can easily see that every diophantine set is recursively enumerable (see the end of section 1.1). However, the converse problem — are recursively enumerable sets diophantine? — is much more difficult.

*The author is a Postdoctoral Fellow of the Research Foundation — Flanders (FWO).
Address: Ghent University, Department of Pure Mathematics and Computer Algebra, Krijgslaan 281, 9000 Gent, Belgium. **E-mail:** jdemeyer@cage.ugent.be.

In 1970, Matiyasevich ([9]) showed, building on earlier work by Davis, Putnam and Robinson, that r.e. sets are diophantine for the integers $\mathbb{Z}$. This had as an immediate consequence the negative answer to Hilbert's Tenth Problem: there exists no algorithm which can decide whether a diophantine equation over $\mathbb{Z}$ has a zero over $\mathbb{Z}$. See [1] for a good write-up of the various steps in the proof that r.e. sets are diophantine for $\mathbb{Z}$, and hence the negative answer to Hilbert's Tenth Problem.

The undecidability of diophantine equations has been shown for many other rings and fields, [12] and [13] give a good overview of what is known. On the other hand, the equivalence of r.e. and diophantine sets is much stronger and much less is known.

Apart from the original result for $\mathbb{Z}$, this equivalence has been shown for $\mathbb{Z}[Z]$ by Denef ([4]), for $\mathcal{O}_K[Z_1, \ldots, Z_n]$ where K is a totally real number field by Zahidi ([16] and [15]). In characteristic p, it is known for $\mathbb{F}_q[Z]$ and for $K[Z]$ where K is a recursive algebraic extension of a finite field by the author ([3]). The latter ring is not recursively stable, so the equivalence is between diophantine sets and sets which are r.e. for every recursive presentation. All these results use the fact that r.e. sets are diophantine for $\mathbb{Z}$. This paper is no exception, however we base ourselves on Denef's result for $\mathbb{Z}[Z]$.

1.1 Definitions

We quickly recall the definitions of recursively enumerable sets, recursive rings and diophantine sets. For more information, we refer to the introductory texts [13] and [12].

Definition. Let $\mathcal{S}$ be a subset of $\mathbb{N}^k$. Then $\mathcal{S}$ is called *recursively enumerable* (r.e.) if there exists an algorithm which prints out elements of $\mathcal{S}$ as it runs, such that all elements of $\mathcal{S}$ are eventually printed at least once. Since $\mathcal{S}$ can be infinite, this algorithm is allowed to run infinitely long and use an unbounded amount of memory.

Since there are only countably many algorithms but uncountably many subsets of $\mathbb{N}^k$, there certainly exist sets which are not recursively enumerable. There also exist sets which are recursively enumerable but whose complement is not. Finite unions, finite intersections, cartesian products and projections $\mathbb{N}^{k+r} \to \mathbb{N}^k$ of recursively enumerable sets are still recursively enumerable.

Definition. Let $\mathcal{R}$ be a countable ring. Then $\mathcal{R}$ is called a *recursive ring* if there exists a bijection $\theta : \mathcal{R} \to \mathbb{N}$ such that the sets

$$\{(\theta(X), \theta(Y), \theta(X+Y)) \in \mathbb{N}^3 \mid X, Y \in \mathcal{R}\} \text{ and } \{(\theta(X), \theta(Y), \theta(XY)) \in \mathbb{N}^3 \mid X, Y \in \mathcal{R}\}$$

are recursively enumerable. In this case, θ is called a *recursive presentation* of $\mathcal{R}$. A recursive ring $\mathcal{R}$ is called *recursively stable* if for any two recursive presentations θ_1 and θ_2, the set $\{(\theta_1(X), \theta_2(X)) \in \mathbb{N}^2 \mid X \in \mathcal{R}\}$ is recursively enumerable.

The intuition of a recursive ring is a ring in which we can effectively compute, it is a ring whose elements can be represented by a computer. The recursive presentation θ gives every element of $\mathcal{R}$ a "code", such that, given the codes of X and Y, we can compute the code of $X+Y$ and of XY. If we have two different recursive presentations θ_1 and θ_2, then an element X of $\mathcal{R}$ has two "codes" $\theta_1(X)$ and $\theta_2(X)$. A ring is recursively stable if and only if $\theta_2(X)$ can be effectively computed from $\theta_1(X)$.

Definition. Let $\mathcal{R}$ be a recursively stable ring with a recursive presentation $\theta : \mathcal{R} \to \mathbb{N}$. Then a subset $\mathcal{S} \subseteq \mathcal{R}^k$ is called *recursively enumerable* if and only if $\theta^{\otimes k}(\mathcal{S})$ is an r.e. subset of $\mathbb{N}^k$.

Intuitively, we can still think of r.e. subsets of $\mathcal{R}^k$ as sets which can be printed by an algorithm (possibly running infinitely long). The requirement that $\mathcal{R}$ is recursively stable implies that the definition of r.e. subsets of $\mathcal{R}^k$ does not depend on the choice of θ. One can prove (see [7]) that every field which is finitely generated over its prime field is recursively stable. Furthermore, a recursive integral domain with a recursively stable fraction field is automatically recursively stable. Since we assumed that $\mathcal{R}$ was recursive we have that $\mathcal{R}$ is recursively stable, hence $\mathcal{R}[Z]$ is recursively stable. To construct an example of a ring which is not recursive, consider any non-r.e. subset $\mathcal{S}$ of $\mathbb{N}$. Now take the localization of $\mathbb{Z}$ where the n-th prime number is inverted if and only if $n \in \mathcal{S}$. This is a non-recursive subring of $\mathbb{Q}$.

Definition. Let $\mathcal{R}$ be an integral domain and $\mathcal{S}$ a subset of $\mathcal{R}^k$. Then $\mathcal{S}$ is called *diophantine* if there exists a polynomial $p(a_1, \ldots, a_k, x_1, \ldots, x_n)$ with coefficients in $\mathcal{R}$ such that

$$\mathcal{S} = \{(a_1, \ldots, a_k) \in \mathcal{R}^k \mid p(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0 \text{ for some } x_1, \ldots, x_n \in \mathcal{R}\}. \tag{1}$$

The polynomial p is called a *diophantine definition* of $\mathcal{S}$. A function $f : \mathcal{R}^m \to \mathcal{R}^n$ is called *diophantine* if the set $\{(\overrightarrow{X}, f(\overrightarrow{X})) \in \mathcal{R}^{m+n} \mid \overrightarrow{X} \in \mathcal{R}^m\}$ is diophantine.

When dealing with decidability questions (analogues of Hilbert's Tenth Problem) it often makes sense to restrict the coefficients of the polynomial p to a subring of $\mathcal{R}$. This is certainly necessary if $\mathcal{R}$ is uncountable. However, if we want to prove that r.e. sets are diophantine, then every singleton in $\mathcal{R}$ needs to be diophantine. Therefore, we might as well assume that we take all of $\mathcal{R}$ as ring of coefficients.

If $\mathcal{R}$ is a recursively stable ring, then every diophantine set is recursively enumerable. To see this, consider a diophantine set $\mathcal{S}$ defined as in (1). Construct an algorithm which tries all possible values $(a_1, \ldots, a_k, x_1, \ldots, x_n) \in \mathcal{R}^{k+n}$ and evaluates $p(a_1, \ldots, a_k, x_1, \ldots, x_n)$. Whenever is zero is found, it prints $(a_1, \ldots, a_k)$. This algorithm will print exactly the set $\mathcal{S}$.

1.2 Overview

Let K be a number field and let $\mathcal{R}$ be a subring of K with fraction field K. In order to prove that r.e. sets are diophantine for $\mathcal{R}[Z]$, the main result is the following from section 3:

Theorem. *Let $\mathcal{R}$ be a noetherian integral domain of characteristic zero such that the degree function $\mathcal{R}[Z] \setminus \{0\} \to \mathbb{Z}$ is diophantine. Then $\mathbb{Z}[Z]$ is a diophantine subset of $\mathcal{R}[Z]$.*

To prove this, we first show that the set of polynomials in $\mathcal{R}[Z]$ which divide some $Z^u - 1$ is diophantine. This is done using a Pell equation, similarly to the definition of powers of Z in [2], Section 4. A polynomial F dividing $Z^u - 1$, normalised such that $F(0) = 1$, has coefficients in $\mathbb{Z}$ if and only if $F(h) \in \mathbb{Z}$ for a sufficiently large number h (depending only on the degree of F). In this way, we diophantinely define the polynomials in $\mathbb{Z}[Z]$ dividing some $Z^u - 1$. We call these the *root-of-unity polynomials*. This set is Z-adically dense in $\mathbb{Z}[[Z]]^*$, which allows us to diophantinely define all of $\mathbb{Z}[Z]$ in $\mathcal{R}[Z]$.

Once we have a diophantine definition of $\mathbb{Z}[Z]$, it follows from [4] that r.e. subsets of $\mathbb{Z}[Z]^k$ are diophantine over $\mathcal{R}[Z]$. From this, the main result for $\mathcal{R}[Z]$ easily follows.

At several points in the proof above we need a diophantine definition of the degree function $\deg : \mathcal{R}[Z] \setminus \{0\} \to \mathbb{Z}$. We give such a diophantine definition in section 4. We apply a result by Kim and Roush who showed in [8] that

diophantine equations over $L(Z)$ are undecidable if L is contained in a finite extension of $\mathbb{Q}_p$ for some $p \geq 3$. They showed undecidability by giving a diophantine definition of the discrete valuation ring $L[Z]_{(Z)}$. Since "negative degree" is a discrete valuation, the same method gives a diophantine definition of "degree" in $\mathcal{R}[Z]$.

2 Special polynomials

In this section, we state some properties of the Chebyshev polynomials X_n and Y_n and cyclotomic polynomials Φ_n. We also define root-of-unity polynomials. Everything in this section concerns only the ring $\mathbb{Z}[Z]$.

2.1 Chebyshev polynomials

Definition 1. Let $n \in \mathbb{Z}$ and define polynomials $\mathrm{X}_n, \mathrm{Y}_n \in \mathbb{Z}[Z]$ using the following equality:

$$(Z + \sqrt{Z^2 - 1})^n = \mathrm{X}_n(Z) + \sqrt{Z^2 - 1}\,\mathrm{Y}_n(Z). \tag{2}$$

Since $(Z + \sqrt{Z^2 - 1})^{-1} = (Z - \sqrt{Z^2 - 1})$, this definition makes sense for negative n.

The degree of X_n is $|n|$; the degree of Y_n is $|n| - 1$ for $n \neq 0$, while $\mathrm{Y}_0 = 0$.

In the literature, X_n is called the n-th Chebyshev polynomial of the first kind and Y_{n+1} is called the n-th Chebyshev polynomial of the second kind (such that the n-th Chebyshev polynomials have degree n for $n \geq 0$).

The couples $(\mathrm{X}_n, \mathrm{Y}_n)$ satisfy the Pell equation $X^2 - (Z^2 - 1)Y^2 = 1$. Conversely, we have:

Proposition 2. *Let $\mathcal{R}$ be an integral domain of characteristic zero and T a non-constant polynomial in $\mathcal{R}[Z]$. If X and Y in $\mathcal{R}[Z]$ satisfy $X^2 - (T^2 - 1)Y^2 = 1$, then $X = \pm\mathrm{X}_n(T)$ and $Y = \mathrm{Y}_n(T)$ for some $n \in \mathbb{Z}$.*

Proof. See [5], Lemma 2.1. Since $\mathrm{X}_{-n} = \mathrm{X}_n$ and $\mathrm{Y}_{-n} = -\mathrm{Y}_n$, we do not need to put $\pm$ in front of $\mathrm{Y}_n(T)$. □

The Chebyshev polynomials also satisfy the following identity:

Proposition 3. *In $\mathbb{Q}(Z)$, the following equality holds for all $n \in \mathbb{Z}$:*

$$Z^n = \mathrm{X}_n\left(\frac{Z+Z^{-1}}{2}\right) + \frac{Z-Z^{-1}}{2}\mathrm{Y}_n\left(\frac{Z+Z^{-1}}{2}\right). \tag{3}$$

Proof. This easily follows from (2). □

2.2 Cyclotomic and root-of-unity polynomials

Let $\Phi_n \in \mathbb{Z}[Z]$ denote the n-th cyclotomic polynomial.

Proposition 4. *Let $n \geq 2$ and write $n = \prod_{i=1}^{k} p_i^{e_i}$, where the p_i's are distinct primes and every $e_i \geq 1$. Let $d := \prod_{i=1}^{k} p_i^{e_i-1}$. Then*

$$\Phi_n(Z) \equiv 1 + (-1)^{k+1} Z^d \pmod{Z^{2d}}.$$

Proof. If μ denotes the Möbius function, then we have

$$\Phi_n(Z) = \prod_{a|n} (Z^{n/a} - 1)^{\mu(a)}.$$

Since $n \geq 2$, we have $\sum_{a|n} \mu(a) = 0$ and we can multiply by $1 = \prod_{a|n}(-1)^{\mu(a)}$ to get:

$$\Phi_n(Z) = \prod_{a|n} (1 - Z^{n/a})^{\mu(a)}.$$

Now we evaluate this product modulo Z^{2d}.

If $n/a \geq 2d$ then $(1 - Z^{n/a})^{\mu(a)}$ is congruent to 1 (mod Z^{2d}). The same happens if a is not squarefree since in this case $\mu(a) = 0$. The only squarefree a dividing n such that $n/a < 2d$ equals $a = n/d$. So we have

$$\Phi_n(Z) \equiv (1 - Z^d)^{\mu(n/d)} \pmod{Z^{2d}}.$$

If k is even, then $\mu(n/d) = 1$ and we have the desired result. If k is odd, then $\mu(n/d) = -1$ and we have $(1 - Z^d)^{-1} = (1 + Z^d)(1 - Z^{2d})^{-1} \equiv 1 + Z^d$ (mod Z^{2d}). □

Corollary 5. *Let $d \in \mathbb{N}$ and $s \in \{-1, 1\}$. Then there exist infinitely many $n \in \mathbb{N}$ such that*

$$\Phi_n(Z) \equiv 1 + sZ^d \pmod{Z^{2d}}.$$

Proof. Write $d := \prod_{i=1}^{k} p_i^{e_i}$ and let $m := \prod_{i=1}^{k} p_i^{e_i+1}$. If r is any squarefree number coprime to m, then it follows from Proposition 4 that $\Phi_{rm}(Z)$ is congruent to $1 \pm Z^d \pmod{Z^{2d}}$, where the sign of Z^d is determined by the parity of the number of factors in rm. Now the statement clearly follows. □

Definition 6. We call a polynomial $F \in \mathbb{Z}[Z]$ a *root-of-unity polynomial* if it satisfies one of the following three equivalent conditions:

1. F is a divisor of $Z^u - 1$ for some $u > 0$.
2. F or $-F$ is a product of distinct cyclotomic polynomials.
3. $F(0) = \pm 1$, F is squarefree and all the zeros of F are roots of unity.

Let $\mathcal{C}$ denote the set of all root-of-unity polynomials, and let $\mathcal{C}^+$ denote those with constant term equal to 1.

Proposition 7. *Let $F \in \mathbb{Z}[Z]$ with $F(0) \in \{-1, 1\}$, and let $d \in \mathbb{Z}_{>0}$. Then there exists a polynomial $M \in \mathcal{C}$ such that $F \equiv M \pmod{Z^d}$.*

If we are working in the Z-adic topology, then "$F \equiv M \pmod{Z^d}$" means that M is an approximation of F with a precision of Z^d. Since the units of $\mathbb{Z}[[Z]]$ are exactly the power series F with $F(0) = \pm 1$, the proposition can be rephrased as follows: *the set of root-of-unity polynomials is Z-adically dense in $\mathbb{Z}[[Z]]^*$.*

Proof. Since the set $\mathcal{C}$ is invariant under changing sign, we may assume without loss of generality that $F(0) = 1$.

The proof will be done by induction on d, which means that we will construct better and better approximations of F. For $d = 1$, we can take $M = 1$. Now let $d \geq 1$ and assume that $F \equiv M_0 \pmod{Z^d}$, where $M_0 \in \mathcal{C}$. Then $F - M_0 \equiv cZ^d \pmod{Z^{d+1}}$ for some $c \in \mathbb{Z}$. If c happens to be zero, then we can take $M = M_0$.

First consider the case $c > 0$. By Corollary 5, we can find an $n_1 \in \mathbb{N}$ such that $\Phi_{n_1}(Z) \equiv 1 + Z^d \pmod{Z^{2d}}$ and such that $\Phi_{n_1}(Z)$ is not a factor of M_0. Let $M_1 := M_0\Phi_{n_1}(Z)$. Since $M_0(0) = 1$, we get

$$F - M_1 \equiv F - M_0(1 + Z^d) \equiv (F - M_0) - M_0 Z^d \equiv (c-1)Z^d \pmod{Z^{d+1}}.$$

We can iterate this procedure. Set $M_2 := M_1\Phi_{n_2}(Z)$ for a Φ_{n_2} which is congruent to $1 + Z^d \pmod{Z^{2d}}$, then $F - M_2 \equiv (c-2)Z^d \pmod{Z^{d+1}}$. After c steps, we have $F - M_c \equiv 0 \pmod{Z^{d+1}}$. So we can take $M := M_c$.

The case $c < 0$ is analogous, the only difference is that we need to multiply with polynomials which are congruent to $1 - Z^d \pmod{Z^{d+1}}$. □

3 Defining polynomials with integer coefficients

Throughout this section, $\mathcal{R}$ is a noetherian integral domain of characteristic zero such that the degree function $\mathcal{R}[Z] \setminus \{0\} \to \mathbb{Z}$ is diophantine. If $\mathcal{R}$ is a subring of a number field, it is a noetherian integral domain of characteristic zero and in section 4 we will show that "degree" is diophantine for such $\mathcal{R}[Z]$. When we say that "degree" is diophantine, we actually mean that the composition $\mathcal{R}[Z] \setminus \{0\} \to \mathbb{Z} \hookrightarrow \mathcal{R}[Z]$ is diophantine. This makes sense since the set $\mathbb{Z}$ is diophantine in $\mathcal{R}[Z]$ (see [14], Theorem 5.1).

In this section, we show that $\mathbb{Z}[Z]$ is a diophantine subset of $\mathcal{R}[Z]$. This is done in three steps: first we diophantinely define all divisors of some $Z^u - 1$ in $\mathcal{R}[Z]$. Second, we restrict these to the polynomials which have integer coefficients, i.e. the root-of-unity polynomials. Third, we use Proposition 7 to get all of $\mathbb{Z}[Z]$ in $\mathcal{R}[Z]$.

3.1 Divisors of $Z^u - 1$

We give a diophantine definition of the divisors of $Z^u - 1$, without requiring that they have coefficients in $\mathbb{Z}$. For technical reasons, we first restrict ourselves to polynomials of degree at least 3.

Lemma 8. *For $G \in \mathcal{R}[Z]$ with $\deg(G) \geq 3$, we have*

$$(\exists u > 0)(G \mid Z^u - 1 \ \wedge \ G(0) = 1) \tag{4}$$

$$\Updownarrow$$

$$(\exists S, X, Y)(X^2 - \Big(\big(\tfrac{Z+S}{2}\big)^2 - 1\Big) Y^2 = 1 \ \wedge \ X \equiv 1 \pmod{Z + S - 2} \tag{5}$$

$$\wedge\, Y \neq 0 \ \wedge \ G = 1 - ZS \ \wedge \ X + \big(\tfrac{Z-S}{2}\big) Y \equiv 1 \pmod{G}) \tag{6}$$

Proof. The formula $(\exists S)(G = 1 - ZS)$ is equivalent to $G(0) = 1$. Since $\deg(G) \geq 3$ and $G = 1 - ZS$, it follows that $\deg(S) \geq 2$. Therefore $Z + S$ is non-constant. By Proposition 2, the first part of formula (5) is equivalent to

$$X = \pm \mathrm{X}_n\big(\tfrac{Z+S}{2}\big) \text{ and } Y = \mathrm{Y}_n\big(\tfrac{Z+S}{2}\big) \text{ for some } n \in \mathbb{Z}.$$

Since $X_n(1) = 1$, the condition $X \equiv 1 \pmod{Z + S - 2}$ forces the sign of X to be positive. The formula $Y \neq 0$ is equivalent to $n \neq 0$.

In the last part of formula (6), we are working modulo $G = 1 - ZS$. But this means that $S \equiv Z^{-1} \pmod{G}$. So, that formula becomes equivalent to

$$\mathrm{X}_n\Big(\tfrac{Z+Z^{-1}}{2}\Big) + \Big(\tfrac{Z-Z^{-1}}{2}\Big) \mathrm{Y}_n\Big(\tfrac{Z+Z^{-1}}{2}\Big) \equiv 1 \pmod{G}.$$

Using Proposition 3, this is equivalent to $Z^n \equiv 1 \pmod{G}$. Without loss of generality, we may assume that $n \geq 0$ (otherwise multiply both sides by Z^{-n}). Then we can rewrite $Z^n \equiv 1 \pmod{G}$ as $G \mid Z^n - 1$. □

Proposition 9. *In $\mathcal{R}[Z]$, the set of all polynomials dividing $Z^u - 1$ for some $u > 0$ is diophantine.*

Proof. Let F be an element of $\mathcal{R}[Z]$. We claim that F divides some $Z^u - 1$ if and only if

$$(\exists G)\big(F \mid G \ \wedge \ (Z^3 - 1) \mid G \ \wedge \ (\exists u > 0)(G \mid Z^u - 1 \ \wedge \ G(0) = 1)\big). \tag{7}$$

If formula (7) is satisfied, then $F \mid G \mid Z^u - 1$. Conversely, if $F \mid Z^u - 1$, we can set $G = \mathrm{lcm}(Z^3 - 1, F)$. Then G will divide $Z^{3u} - 1$. Since F divides $Z^u - 1$, its constant coefficient must be a unit, therefore G can be chosen to have $G(0) = 1$.

Applying Lemma 8, we see that (7) is diophantine. Indeed, a congruence $A \equiv B \pmod{C}$ can be written as $(\exists X)(A - B = CX)$. The formula $Y \neq 0$ is diophantine using the fact that $\mathcal{R}[Z]$ is noetherian (see [11], Théorème 3.1). Hence, formulas (5)–(6) are diophantine. We can apply Lemma 8 because the G appearing in (7) must have degree ≥ 3. □

3.2 Root-of-unity polynomials

Now we have a diophantine definition of the divisors of $Z^u - 1$, but we only want those divisors with integer coefficients. We take care of this using the following proposition, which was inspired by [4] and [16].

Proposition 10. *Let K be a number field and $\mathcal{O}$ its ring of integers. Let $F \in \mathcal{O}[Z]$ be a polynomial satisfying $F(0) \in \{-1, 1\}$ whose zeros (over an algebraic closure) are all roots of unity. If $F(2^{\deg F} + 1)$ is an integer, then every coefficient of F is an integer.*

Proof. By changing sign if necessary, we may assume without loss of generality that $F(0) = 1$. Let d be the degree of F and write

$$F(Z) = \sum_{i=0}^{d} \alpha_i Z^i, \tag{8}$$

where $\alpha_i \in \mathcal{O}$. Note that $\alpha_d \neq 0$ and $\alpha_0 = 1$.

If $d = 0$, then $F(Z) = 1$ which is in $\mathbb{Z}[Z]$. Now assume that $d \geq 1$. Over an algebraic closure, F can be factored as

$$F(Z) = \alpha_d (Z - \zeta_1) \dots (Z - \zeta_d), \tag{9}$$

where every ζ_i is a root of unity. We see that $F(0) = \alpha_d (-1)^d \prod_{i=1}^{d} \zeta_i$. This must be equal to 1, therefore α_d is also a root of unity. Write $\sigma_{d,i}$ for the i-th elementary symmetric polynomial in d variables. Since $\sigma_{d,i}$ has $\binom{d}{i}$ terms, it follows that $\alpha_i = \alpha_d \cdot \sigma_{d,i}(\zeta_1, \dots, \zeta_d)$ is the sum of $\binom{d}{i}$ roots of unity.

Let $|\cdot|$ be an archimedean absolute value on K (i.e. an absolute value coming from an embedding $K \hookrightarrow \mathbb{C}$). Then we have $|\alpha_i| \leq \binom{d}{i}$. Since $\binom{d}{i} \leq 2^{d-1}$ for all $d \geq 1$ and all $i \in \{0, \dots, d\}$, we have $|\alpha_i| \leq 2^{d-1}$.

Define the set $\mathcal{G}_d \subseteq \mathcal{O}[Z]$ consisting of all polynomials $G \in \mathcal{O}[Z]$ satisfying:

1. The degree of G is at most d.
2. $G(2^d + 1)$ is an integer.
3. $|\gamma_i| \leq 2^{d-1}$ for every coefficient γ_i of G and every archimedean absolute value on K.

Clearly, the elements of $\mathbb{Z}[Z]$ having degree at most d and coefficients in the interval $\{-2^{d-1}, \ldots, 2^{d-1}\}$ are in $\mathcal{G}_d$. There are $(2^d+1)^{d+1}$ such polynomials. We claim that these are the only elements of $\mathcal{G}_d$. Since F is in $\mathcal{G}_d$, this claim implies the proposition.

To prove the claim, take any G in $\mathcal{G}_d$ and write $G = \sum_{i=0}^{d} \gamma_i Z^i$ (where we allow $\gamma_d = 0$). We have the following bound for all $h \in \mathbb{Z}$ with $h > 1$:

$$|G(h)| \leq \sum_{i=0}^{d} |\gamma_i| h^i \leq 2^{d-1} \frac{h^{d+1} - 1}{h - 1}.$$

Fix $h := 2^d + 1$ for the remainder of this proof. Then we have $|G(h)| \leq (h^{d+1} - 1)/2$.

Now take two elements $G \neq H$ in $\mathcal{G}_d$ and let $D := G - H$. Write $D(Z) = \sum_{i=0}^{e} \delta_i Z^i$ with $\delta_e \neq 0$ (clearly, $e \leq d$). We want to prove that $D(h) \neq 0$, so assume that $D(h) = 0$. Then

$$\delta_e h^e = -\sum_{i=0}^{e-1} \delta_i h^i. \tag{10}$$

The coefficients of G and H have absolute value at most 2^{d-1}, therefore $|\delta_i| \leq 2^d$. Since $\delta_e \in \mathcal{O}$ is integral over $\mathbb{Z}$, we have $|\delta_e|_{\mathfrak{p}} \leq 1$ for every non-archimedean ($\mathfrak{p}$-adic) absolute value on K. From the product formula for absolute values it follows that $|\delta_e| \geq 1$ for some archimedean absolute value on K. If we take such an absolute value, then (10) implies the following contradiction:

$$h^e \leq |\delta_e h^e| \leq \sum_{i=0}^{e-1} |\delta_i| h^i \leq 2^d \frac{h^e - 1}{h - 1} = h^e - 1.$$

Consider again the set $\mathcal{G}_d$. We just showed that $G(h)$ cannot take the same value for two different elements G in $\mathcal{G}_d$. Since $G(h) \in \mathbb{Z}$ by definition of $\mathcal{G}_d$ and $|G(h)| \leq (h^{d+1} - 1)/2$, it follows that $\mathcal{G}_d$ has at most h^{d+1} elements. But we already know that there are h^{d+1} elements in $\mathcal{G}_d \cap \mathbb{Z}[Z]$, therefore $\mathcal{G}_d \subseteq \mathbb{Z}[Z]$. □

Taking Propositions 9 and 10 together, we can now prove:

Proposition 11. *If "degree" is diophantine in $\mathcal{R}[Z]$, then the set $\mathcal{C}$ is a diophantine subset of $\mathcal{R}[Z]$.*

Proof. The $\mathcal{R}[Z]$-divisors of $Z^u - 1$ are diophantine by Proposition 9. If we take only those polynomials with $F(0) = \pm 1$, they satisfy the conditions of Proposition 10 with $K = \mathbb{Q}(\zeta_u)$ where ζ_u is a primitive u-th root of unity. Note that $F(0) \in \{-1, 1\}$ is equivalent to $Z \mid F^2 - 1$, a diophantine condition. The formula

$$(\exists t \in \mathbb{Z})\big(F \equiv t \pmod{Z - 2^{\deg(F)} - 1}\big) \tag{11}$$

expresses that F evaluated at $2^{\deg(F)} + 1$ is an integer. Since $\mathbb{Z}$ is diophantine in $\mathcal{R}[Z]$ (see [14], Theorem 5.1) and "degree" is diophantine by assumption, formula (11) is diophantine. □

3.3 All polynomials with integer coefficients

Proposition 11 gives us a diophantine definition of $\mathcal{C}$, which is a subset of $\mathbb{Z}[Z]$. To define all of $\mathbb{Z}[Z]$ in $\mathcal{R}[Z]$, we use Proposition 7. By taking remainders of the elements of $\mathcal{C}$ after Euclidean division by Z^d, we get all elements of $\mathbb{Z}[Z]$ with constant coefficient 1 or -1. We don't actually need that the set of powers of Z is diophantine, we can divide by elements of $\mathcal{C} + 1$, which contains the powers of Z. In order for Euclidean division to be diophantine, we need "degree" to be diophantine. To get all elements of $\mathbb{Z}[Z]$, we just need to add an integer to the polynomials we get as remainders.

Theorem 12. *Let $\mathcal{R}$ be a noetherian integral domain of characteristic zero such that "degree" is diophantine. Then $\mathbb{Z}[Z]$ is a diophantine subset of $\mathcal{R}[Z]$.*

Proof. Let X be an element of $\mathcal{R}[Z]$. We claim that X is in $\mathbb{Z}[Z]$ if and only if

$$(\exists M, D, Q, R, C)(M \in \mathcal{C} \ \wedge \ D \in \mathcal{C} \ \wedge \ (Z - 1) \mid D \tag{12}$$

$$\wedge \ M = Q(D + 1) + R \ \wedge \ (R = 0 \ \vee \ \deg(R) < \deg(D)) \tag{13}$$

$$\wedge \ C \in \mathbb{Z} \ \wedge \ X = R + C). \tag{14}$$

Assume that X is indeed in $\mathbb{Z}[Z]$. Then set $C := X(0) - 1$ and $R := X - C$ such that $R(0) = 1$. Let $D := Z^{\deg(R)+1} - 1$. Apply Proposition 7 to find an $M \in \mathcal{C}$ such that $R \equiv M \pmod{D + 1}$ and let $Q := (M - R)/(D + 1)$. Now it is clear that (12)–(14) is satisfied.

Conversely, assume that (12)–(14) is satisfied, we have to show that $X \in \mathbb{Z}[Z]$. Since $\mathcal{C} \subseteq \mathbb{Z}[Z]$, we know that M and D are in $\mathbb{Z}[Z]$. The condition

$Z - 1 \mid D$ prevents D from being constant (note that 0 is not an element of $\mathcal{C}$). Since all elements of $\mathcal{C}$ are monic up to sign, $D + 1$ is also. Formula (13) says that R is the remainder of the Euclidean division of M by $D + 1$, therefore $R \in \mathbb{Z}[Z]$. Since $C \in \mathbb{Z}$, it also follows that $X \in \mathbb{Z}[Z]$. □

4 Diophantine definition of degree

We start with a lemma which shows that defining the degree function $\mathcal{R}[Z] \setminus \{0\} \to \mathbb{Z}$ is equivalent to defining a certain "weak" degree equality relation.

Lemma 13. *Let $\mathcal{R}$ be an integral domain of characteristic zero. Let $\delta(F, X)$ be a diophantine relation on $\mathcal{R}[Z]^2$ such that $\delta(F, X)$ is equivalent to $\deg(F) = \deg(X)$ for all $F \in \mathcal{R}[Z] \setminus \{0\}$ and $X \in \mathbb{Z}[Z] \setminus \{0\}$. Then the relation "$\deg(F) = d$" between $F \in \mathcal{R}[Z] \setminus \{0\}$ and $d \in \mathbb{Z}_{\geq 0}$ is diophantine.*

Proof. Let $F \in \mathcal{R}[Z] \setminus \{0\}$ and let $d \in \mathbb{Z}_{\geq 0}$. We claim that F has degree d if and only if

$$(\exists X, Y)(X^2 - (Z^2 - 1)Y^2 = 1 \ \wedge \ Y(1) = d \ \wedge \ \delta(F, X)). \tag{15}$$

Since δ is diophantine and $Y(1) = d$ is equivalent to $Z - 1 \mid Y - d$, this formula is clearly diophantine.

Assume that (15) is satisfied. Since $\mathrm{Y}_n(1) = n$ for any $n \in \mathbb{Z}$, the subformula "$X^2 - (Z^2 - 1)Y^2 = 1 \ \wedge \ Y(1) = d$" is equivalent to "$X = \pm \mathrm{X}_d(Z) \ \wedge \ Y = \mathrm{Y}_d(Z)$" by Proposition 2. In particular, X is an element of $\mathbb{Z}[Z]$ of degree d. By the assumptions on δ, this implies that $\deg(F) = d$.

Conversely, if the degree of F equals d, then we set $X = \mathrm{X}_d(Z)$ and $Y = \mathrm{Y}_d(Z)$. This satisfies (15). □

As in the Introducion, let K be a number field and $\mathcal{R}$ a subring of K with fraction field K.

To diophantinely define degree in $\mathcal{R}[Z]$, we use the fact that "negative degree" is a discrete valuation on $K(Z)$. More precisely, if $F, G \in \mathcal{R}[Z]$, then $v_{Z^{-1}}(F/G) := \deg(G) - \deg(F)$ defines a discrete valuation on $K(Z)$. Therefore, the problem reduces to showing that the discrete valuation ring at Z^{-1} in $K(Z)$ is diophantine. For this, we need certain quadratic forms used by

Kim and Roush (see [8]) to prove undecidability for rational function fields over so-called p-adic fields with p odd. This undecidability has been generalised to arbitrary function fields over p-adic fields with p odd (see [10] or [6]).

Definition 14. Let p be a prime number. A field K is called *p-adic* if K can be embedded in a finite extension of $\mathbb{Q}_p$.

It is clear from this definition that every number field is p-adic for every p. For the rest of this section, we fix any odd prime p. Following the method by Kim and Roush, we need to work over a field satisfying Hypothesis $(\mathcal{H})$.

Definition 15. Let L be a p-adic field with p odd and let $v_{\mathfrak{p}}$ be a discrete valuation on L extending the p-adic valuation on $\mathbb{Q}$. We say that L satisfies Hypothesis $(\mathcal{H})$ if and only if L contains elements α and π such that

1. $v_{\mathfrak{p}}(\pi)$ is odd and π is algebraic over $\mathbb{Q}$.
2. α is a root of unity.
3. L contains a square root of -1.
4. The quadratic form $\langle 1, \alpha\rangle\langle 1, \pi\rangle$ is anisotropic (i.e. has no non-trivial zeros) in the completion $L_{\mathfrak{p}}$.
5. The quadratic form $\langle 1, \alpha\rangle\langle 1, \pi\rangle$ is isotropic in all 2-adic completions of $\mathbb{Q}(\alpha, \pi, \sqrt{-1})$.

Proposition 16 ([8], Proposition 8)**.** *Let K be a p-adic field for an odd prime p. Then there exists a finite extension L of K which satisfies Hypothesis $(\mathcal{H})$.*

The next two propositions deal with certain quadratic forms. Our variable Z is the inverse of the variable t that Kim and Roush use.

Proposition 17 ([8], Proposition 7)**.** *Let L be any field of characteristic 0 and suppose that $\langle 1, -\alpha\rangle\langle 1, \pi\rangle$ is an anisotropic quadratic form over L. Let $F \in L(Z)$ such that $v_{Z^{-1}}(F)$ is non-negative and even. Then one of the following two is anisotropic over $L(Z)$:*

$$\langle Z, -\alpha Z, -1, -F\rangle\langle 1, \pi\rangle \tag{16}$$

$$\langle Z, -\alpha Z, -1, -\alpha F\rangle\langle 1, \pi\rangle. \tag{17}$$

The following proposition follows from [8]. However, here we use a reformulation by Eisenträger (see [6], Theorem 8.1). Note that the condition that G has algebraic coefficients is missing from Eisenträger's paper, but it is necessary and it does appear in Kim and Roush.

Proposition 18. *Let L be a p-adic field satisfying Hypothesis $(\mathcal{H})$ for elements α and π in L. Let $\mathcal{U} \subseteq L(Z)$ such that $\mathcal{U} \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_m}$ for every finite set of rational primes $\{p_1, \ldots, p_m\}$. Let $G \in L(Z)$ such that $v_Z(G) = -2$ and $v_{Z^{-1}}(G) = 1$. Assume that $G = G_N(Z)/G_D(Z)$ for polynomials G_N and G_D with coefficients algebraic over $\mathbb{Q}$. Then there exist $\gamma_3, \gamma_5 \in \mathcal{U}$ such that, if we let*

$$F := (1 + Z^{-1})^3 G(Z) + \gamma_3 Z^{-3} + \gamma_5 Z^{-5}, \tag{18}$$

then the following quadratic forms are both isotropic over $L(Z)$:

$$\langle Z, \alpha Z, -1, -F \rangle \langle 1, \pi \rangle \tag{19}$$

$$\langle Z, \alpha Z, -1, -\alpha F \rangle \langle 1, \pi \rangle. \tag{20}$$

The most natural choice for $\mathcal{U}$ would be $\mathcal{U} = L$. However, for our applications, $\mathcal{U}$ needs to be diophantine in $L(Z)$. In the article by Kim and Roush, $\mathcal{U}$ is a subset of L. However, since enlarging the set $\mathcal{U}$ only weakens the proposition, we can even take $\mathcal{U}$ in $L(Z)$.

Taking these last two propositions together, we can prove the following:

Proposition 19. *Let L and $\mathcal{U}$ be as in Proposition 18 with the additional condition that every element $A \in \mathcal{U}$ has $v_{Z^{-1}}(A) \geq 0$. Let $X \in L(Z)$ with algebraic coefficients and define*

$$G(Z) := \frac{(Z + Z^2) + X^3}{Z^3 + Z^2 X^3}.$$

Then $v_{Z^{-1}}(X) \geq 0$ if and only if there exist $\gamma_3, \gamma_5 \in \mathcal{U}$ such that the quadratic forms (19) and (20) are both isotropic with F as in (18).

Proof. Write $G_N := (Z + Z^2) + X^3$ and $G_D := Z^3 + Z^2 X^3$ such that $G = G_N/G_D$. Assume that $v_{Z^{-1}}(X) \geq 0$. Then $v_{Z^{-1}}(G_N) = -2$ and $v_{Z^{-1}}(G_D) = -3$, such that $v_{Z^{-1}}(G) = 1$. If $v_Z(X) \geq 1$, then $v_Z(G_N) = 1$ and $v_Z(G_D) = 3$, such that $v_Z(G) = -2$. If $v_Z(X) \leq 0$, then $v_Z(G_N) = 3v_Z(X)$ and $v_Z(G_D) = 2 + 3v_Z(X)$, such that $v_Z(G) = -2$. Summarized, if $v_{Z^{-1}}(X) \geq 0$, then we

have $v_{Z^{-1}}(G) = 1$ and $v_Z(G) = -2$. Proposition 18 gives us that (19) and (20) are indeed isotropic for some choice of γ_3 and γ_5 in $\mathcal{U}$.

Conversely, assume that $v_{Z^{-1}}(X) < 0$. We must show that one of the forms (19) or (20) is anisotropic for every γ_3, γ_5 with non-negative valuation at Z^{-1}. Since $v_{Z^{-1}}(X) \leq -1$, we have $v_{Z^{-1}}(G_N) = 3v_{Z^{-1}}(X)$ and $v_{Z^{-1}}(G_D) = -2 + 3v_{Z^{-1}}(X)$. Therefore $v_{Z^{-1}}(G) = 2$. Since $v_{Z^{-1}}(\gamma_i) \geq 0$, it follows from (18) that $v_{Z^{-1}}(F) = 2$. Hypothesis $(\mathcal{H})$ says that $\langle 1, \alpha\rangle\langle 1, \pi\rangle$ is locally anisotropic at $\mathfrak{p}$, hence it is also globally anisotropic over L. Since L contains $\sqrt{-1}$, signs in quadratic forms do not matter. Therefore, we can apply Proposition 17. □

Theorem 20. *Let $\mathcal{R}$ be a subfield of a number field K with fraction field K. In the ring $\mathcal{R}[Z]$, the relation "$\deg(X) = d$" between $X \in \mathcal{R}[Z] \setminus \{0\}$ and $d \in \mathbb{Z}_{\geq 0}$ is diophantine.*

Proof. Let $X, Y \in \mathcal{R}[Z] \setminus \{0\}$. If we can give a diophantine definition of "$\deg(X) \leq \deg(Y)$", then "$\deg(X) \leq \deg(Y) \ \wedge \ \deg(Y) \leq \deg(X)$" is a predicate $\delta(X, Y)$ which satisfies the conditions of Lemma 13.

Since the non-zero elements of $\mathcal{R}[Z]$ form a diophantine subset of $\mathcal{R}[Z]$ (see [11]), we can construct a diophantine interpretation of the fraction field $K(Z)$ over $\mathcal{R}[Z]$. Let L be a finite extension of K which satisfies Hypothesis $(\mathcal{H})$. Using a basis of L as a K-vector space, there is a diophantine model of $L(Z)$ over $K(Z)$.

Since $\deg(X) \leq \deg(Y)$ is equivalent to $v_{Z^{-1}}(X/Y) \geq 0$, it suffices to give a diophantine definition of the predicate "$v_{Z^{-1}}(X) \geq 0$" with $X \in L(Z)$. Let

$$\mathcal{U} = \{n/P \mid n \in \mathbb{Z} \ \wedge \ P \in \mathcal{R}[Z] \setminus \{0\}\} \subseteq K(Z).$$

By construction, every element $A \in \mathcal{U}$ has $v_{Z^{-1}}(A) \geq 0$. The set $\mathcal{U}$ contains $\mathbb{Q}$, which is clearly dense in every $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_m}$. Since quadratic forms being isotropic is a diophantine condition and $\mathcal{U}$ is diophantine, it follows by Proposition 19 that "$v_{Z^{-1}}(X) \geq 0$" is diophantine. □

5 Recursively enumerable sets

In this final section we discuss how having a diophantine definition of $\mathbb{Z}[Z]$ in $\mathcal{R}[Z]$ gives us that r.e. subsets of $\mathcal{R}[Z]^k$ are diophantine. Recall that $\mathcal{R}$ is a subring of a number field K with fraction field K.

Denef showed (see [4]) that r.e. subsets of $\mathbb{Z}[Z]^k$ are diophantine over $\mathbb{Z}[Z]$. Since we showed in the preceding sections that $\mathbb{Z}[Z]$ is a diophantine subset of $\mathcal{R}[Z]$, it also follows that r.e. subsets of $\mathbb{Z}[Z]^k$ are diophantine over $\mathcal{R}[Z]$.

Let $\alpha \in \mathcal{R}$ such that $K = \mathbb{Q}(\alpha)$ and let $d := [K : \mathbb{Q}]$. Now any element X of $\mathcal{R}[Z]$ can be written as

$$X = \frac{X_0 + X_1\alpha + \cdots + X_{d-1}\alpha^{d-1}}{y} \tag{21}$$

with X_i in $\mathbb{Z}[Z]$ and y in $\mathbb{Z} \setminus \{0\}$.

Now let $\mathcal{S} \subseteq \mathcal{R}[Z]$ be an r.e. set, we have to show that $\mathcal{S}$ is diophantine. To $\mathcal{S}$ we associate a set $\mathcal{T} \subseteq \mathbb{Z}[Z]^{d+1}$ using (21): the set $\mathcal{T}$ has one tuple $(X_0, X_1, \ldots, X_{d-1}, y) \in \mathbb{Z}[Z]^{d+1}$ for every $X \in \mathcal{S}$. This tuple $(X_0, X_1, \ldots, X_{d-1}, y)$ is not unique but that is not a problem, we can for example try all possible tuples and take the first one which works for a given X. This way, we have a bijection between $\mathcal{S}$ and $\mathcal{T}$. Moreover, the set $\mathcal{T}$ will also be r.e., since we can construct $\mathcal{T}$ from $\mathcal{S}$ using a recursive procedure. Since $\mathcal{T}$ is a subset of $\mathbb{Z}[Z]^{d+1}$, it will be diophantine over $\mathcal{R}[Z]$. Now it immediately follows that $\mathcal{S}$ is diophantine:

$$X \in \mathcal{S} \iff \big(\exists (X_0, X_1, \ldots, X_{d-1}, y) \in \mathcal{T}\big)\big(Xy = X_0 + X_1\alpha + \cdots + X_{d-1}\alpha^{d-1}\big).$$

The argument for sets $\mathcal{S} \subseteq \mathcal{R}[Z]^k$ is very similar, using a set $\mathcal{T} \subseteq \mathbb{Z}[Z]^{(d+1)k}$.

References

[1] Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), no. 3, 233–269.

[2] Jeroen Demeyer, *Recursively enumerable sets of polynomials over a finite field*, J. Algebra **310** (2007), no. 2, 801–828.

[3] ———, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Invent. Math. **170** (2007), no. 3, 655–670.

[4] Jan Denef, *Diophantine sets over* $\mathbb{Z}[T]$, Proc. Amer. Math. Soc. **69** (1978), no. 1, 148–150.

[5] ———, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78 (M. Boffa, D. van Dalen, and K. Mcaloon, eds.), Studies in logic and the foundations of mathematics, no. 97, North-Holland, 1979, pp. 131–145.

[6] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields*, J. Algebra **310** (2007), no. 2, 775–792.

[7] A. Fröhlich and C. Shepherdson, *Effective procedures in field theory*, Phil. Trans. Roy. Soc. London **248** (1956), 407–432.

[8] Ki Hang Kim and Fred Roush, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), no. 1, 83–110.

[9] Yuri Matiyasevich, *Enumerable sets are Diophantine*, Soviet Math. Dokl. **11** (1970), 354–358.

[10] Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, J. Reine und Angew. Math. **587** (2005), 77–143.

[11] ———, *Sur la définissabilité existentielle de la non-nullité dans les anneaux*, Algebra & Number Theory **1** (2007), no. 3, 331–346.

[12] Thanases Pheidas and Karim Zahidi, *Undecidability of existential theories of rings and fields: a survey*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (Denef et al., eds.), Contemp. Math., vol. 270, 2000, pp. 49–105.

[13] Bjorn Poonen, *Undecidability in number theory*, Notices of the AMS **55** (2008), no. 3, 344–350.

[14] Alexandra Shlapentokh, *Diophantine definitions for some polynomial rings*, Commun. Pure Appl. Math. **43** (1990), 1055–1066.

[15] Karim Zahidi, *Existential undecidability for rings of algebraic functions*, Ph.D. thesis, Ghent University, 1999.

[16] ———, *On diophantine sets over polynomial rings*, Proc. Amer. Math. Soc. **128** (2000), no. 3, 877–884.